

2023 年度年次報告書
社会変革に向けた ICT 基盤強化
2022 年度採択研究代表者

藤木 大地

東京工業大学 科学技術創成研究院
准教授

メモリ駆動形 DB システムによるデータ処理基盤強化

研究成果の概要

従来のメモリ中心型計算(PIM)では、頻繁にアクセスされるデータに高速にアクセス機構がないため、局所性の利活用が困難である。特に、データベースのような入力依存なメモリアクセスでは性能課題が生じる。そこで、メモリの複数階層に PIM を設置することで、局所性利活用が可能になることと、その中で階層間のデータ一貫性を保証する「入力コヒーレンス」と「出力コヒーレンス」が重要であることが判明した。本研究では、メモリの見方を透過的に変える「ビュー」を定義し、PIM を非破壊的なビュー生成に限定することで、ビューの入出力コヒーレンスを保証するキャッシュコヒーレンスプロトコルの拡張を定義した。これにより、ビューの再利用が可能となり、汎用インメモリ計算の可能性が広がった。本研究は、計算機アーキテクチャのトップ国際会議 MICRO に採録された¹⁾。

キーバリュー分離型データベースは、LSM 木の課題を解決できる可能性があるが、範囲クエリなどの読み込み操作において性能課題がある。本研究では、セグメント範囲を動的・適応的に調整するシャーディングを考案した。シャード変更時のデータ移動コストを最小化するため、GC 時のデータ移動とリシャーディングをオーバーラップさせる手法を開発した。本研究では、SharK というキーバリューストアエンジンを提案した。これにより、更新性能、読込性能、メモリ効率の三面で効率的なキーバリューストアに一步近づいた。

また、秘密計算を用いた安全なデータベースアクセスを実現する 2 者間秘密文字列一致検索プロトコルを開発した。Learned Index(LI)を準同形暗号に応用し、キー検索の高速化を目指した。プロトコルでは、LI、階層的二分探索、準同形回帰演算を組み合わせ、加法準同形暗号と秘密回転を用いて安全性を確保する。大小比較には、スレッショルド付き準同形暗号と ElGamal 暗号を融合させた新たな暗号を開発し、安全な二分探索のために秘密二分探索プロトコルも開発した。

【代表的な原著論文情報】

- 1) Fujiki, Daichi. "MVC: Enabling Fully Coherent Multi-Data-Views through the Memory Hierarchy with Processing in Memory." In *Proceedings of the 56th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO)*, pp. 800-814. 2023.